



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000196582 A**

(43) Date of publication of application: 14 . 07 . 00

(51) Int. Cl.

H04L 9/08
G06F 12/14
G09C 1/00

(21) Application number: **10371529**

(22) Date of filing: 25 . 12 . 98

(71) Applicant: **NIPPON TELEGR & TELEPH
CORP <NTT>**

(72) Inventor:
UENO MASAMI
SONEOKA AKINAO
MIYAKE NOBUHISA
IORI SACHIKO
ARITA KAZUO

**(54) METHOD FOR RECORDING, UTILIZING AND
 INFORMATION FOR PREVENTING ILLEGAL USE
 BY EMPLOYING STORAGE MEDIA IDENTIFIER**

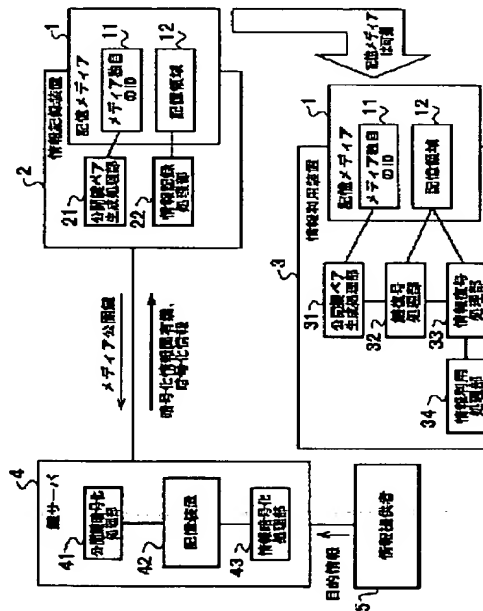
unique to the media and extracts object information.

COPYRIGHT: (C)2000,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method for recording, utilizing and delivering information for preventing illegal use by employing a storage medium identifier where the identifier unique to the storage media is used and the identifier cannot be used even when it is copied to other storage media.

SOLUTION: A key server 4 uses an information specific key to encrypt object information, a storage device 42 stores encrypted information and the information specific key, an information recorder 2 uses an ID 11 unique to a storage media 1 to generate a medium public key and a media secret key and delivers the media public key to the server 4. The server 4 delivers an encrypted information specific key resulting from encrypting the information specific key with the media public key and the encryption information to the information recorder 2, which records the encrypted information specific key and the encrypted information to the storage media 1. An information utilizing device 3 decodes the encrypted information by using the information specific key obtained by decoding the encrypted information specific key with the medium private key generated from the ID 11



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-196582

(43)Date of publication of application : 14.07.2000

(51)Int. Cl.

H04L 9/08

G06F 12/14

G09C 1/00

(21)Application number : 10-371529

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

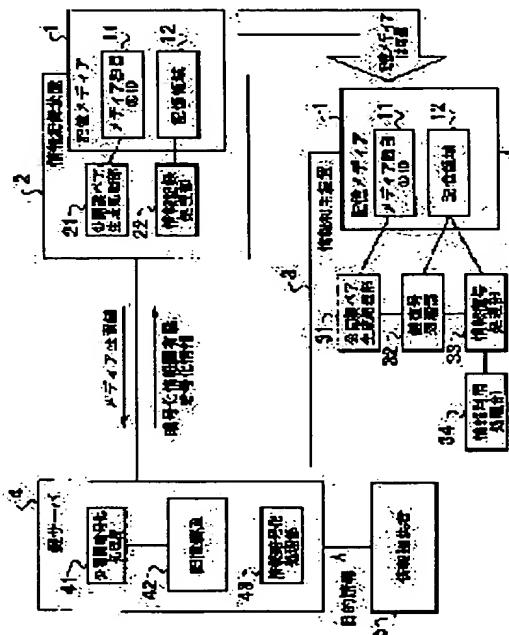
(22)Date of filing : 25.12.1998

(72)Inventor : UENO MASAMI
SONEOKA AKINAO
MIYAKE NOBUHISA
IORI SACHIKO
ARITA KAZUO(54) METHOD FOR RECORDING, UTILIZING AND INFORMATION FOR PREVENTING ILLEGAL USE
BY EMPLOYING STORAGE MEDIA IDENTIFIER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for recording, utilizing and delivering information for preventing illegal use by employing a storage medium identifier where the identifier unique to the storage media is used and the identifier cannot be used even when it is copied to other storage media.

SOLUTION: A key server 4 uses an information specific key to encrypt object information, a storage device 42 stores encrypted information and the information specific key, an information recorder 2 uses an ID 11 unique to a storage media 1 to generate a medium public key and a media secret key and delivers the media public key to the server 4. The server 4 delivers an encrypted information specific key resulting from encrypting the information specific key with the media public key and the encryption information to the information recorder 2, which records the encrypted information specific key and the encrypted information to the storage media 1. An information utilizing device 3 decodes the encrypted information by using the information specific key obtained by decoding the encrypted information specific key with the medium private key generated from the ID 11 unique to the media and extracts object information.



LEGAL STATUS

[Date of request for examination] 17.04.2001

[Date of sending the examiner's decision
of rejection]

[Kind of final disposal of application
other than the examiner's decision of
rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-196582

(P 2 0 0 0 - 1 9 6 5 8 2 A)

(43) 公開日 平成12年7月14日(2000.7.14)

(51) Int. Cl. 7	識別記号	F I	テ-マ-ド (参考)		
H04L 9/08		H04L 9/00	601	B	5B017
G06F 12/14	320	G06F 12/14	320	B	5J104
G09C 1/00	620	G09C 1/00	620	Z	9A001
	630		630	B	
	660		660	A	

審査請求 未請求 請求項の数12 O L (全15頁)

(21) 出願番号 特願平10-371529
(22) 出願日 平成10年12月25日(1998.12.25)

(71) 出願人 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72) 発明者 上野 正巳
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内
(72) 発明者 曾根岡 昭直
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内
(74) 代理人 100083806
弁理士 三好 秀和 (外1名)

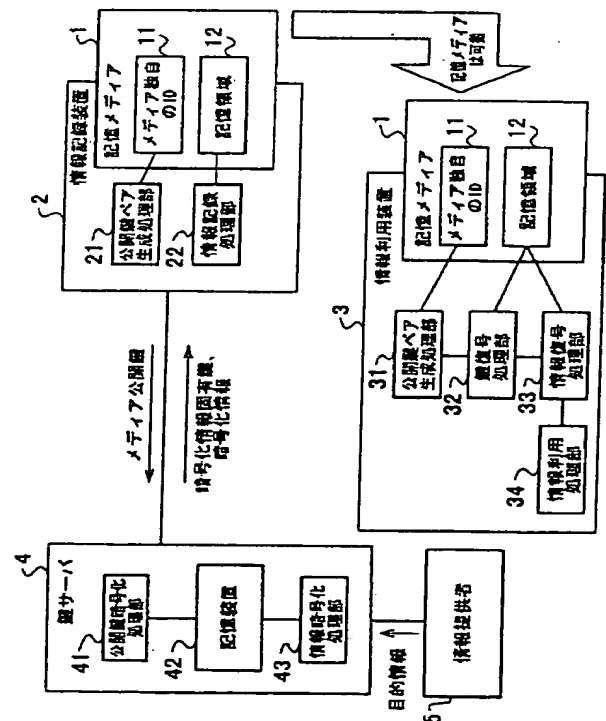
最終頁に続く

(54) 【発明の名称】 記憶メディア識別子を利用した不正利用防止のための情報記録、利用および配送方法

(57) 【要約】

【課題】 記憶メディア独自の識別子を利用し、他の記憶メディアに複製しても利用できないようにした記憶メディア識別子を利用した不正利用防止のための情報記録、利用および配送方法を提供する。

【解決手段】 鍵サーバ4で情報固有鍵で目的情報を暗号化し、暗号化情報と情報固有鍵を記憶装置42に記憶し、情報記録装置2で記憶メディア1独自のID11を用いてメディア公開鍵とメディア秘密鍵を生成し、メディア公開鍵をサーバ4に配送し、サーバ4はメディア公開鍵で情報固有鍵を暗号化した暗号化情報固有鍵と暗号化情報を情報記録装置2に配送し、暗号化情報固有鍵と暗号化情報を記憶メディア1に記録し、情報利用装置3ではメディア独自のID11から生成したメディア秘密鍵で暗号化情報固有鍵を復号して取り出した情報固有鍵で暗号化情報を復号して目的情報を取り出す。



【特許請求の範囲】

【請求項 1】 書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、

不正利用を防止したい目的情報に対して情報固有鍵を生成し、この情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、

前記情報固有鍵を前記メディア公開鍵で暗号化した暗号化情報固有鍵を生成し、

前記暗号化情報と前記暗号化情報固有鍵を記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報記録方法。

【請求項 2】 書換え不可能な独自の識別子を有する記憶メディアに記録された情報の利用を行う情報利用方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、

不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と前記情報固有鍵を前記メディア公開鍵で暗号化した暗号化情報固有鍵を記録している前記記憶メディアから前記暗号化情報固有鍵を読み出し、

この読み出した暗号化情報固有鍵を前記メディア秘密鍵で復号して、情報固有鍵を取り出し、

前記暗号化情報を前記記憶メディアから読み出し、この暗号化情報を前記情報固有鍵で復号して前記目的情報を取り出して利用することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報利用方法。

【請求項 3】 サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と情報固有鍵をサーバ記憶装置に蓄積し、この蓄積されている暗号化情報と情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、

サーバにおいて前記メディア公開鍵で前記情報固有鍵を暗号化して暗号化情報固有鍵を生成し、

前記暗号化情報固有鍵と前記暗号化情報を情報記録装置に送信し、

情報記録装置は前記暗号化情報固有鍵と前記暗号化情報を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。

【請求項 4】 情報提供側からの目的情報を情報利用側に配送し、書換え不可能な独自の識別子を有する記憶メ

ディアに目的情報を記録し、この記録された目的情報を利用する情報の配送、記録および利用方法であって、情報提供側において、前記目的情報に対して情報固有鍵を生成し、この生成した情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、この暗号化情報と前記情報固有鍵を記憶しておく、

情報利用側において、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵を情報提供側に配送し、

情報提供側において、前記メディア公開鍵を受信し、このメディア公開鍵で前記情報固有鍵を暗号化した暗号化情報固有鍵を生成し、この生成した暗号化情報固有鍵と前記暗号化情報を情報利用側に配送し、

情報利用側において、前記暗号化情報固有鍵と前記暗号化情報を受信し、この受信した暗号化情報固有鍵と暗号化情報を前記記憶メディアに記録し、

情報利用側において、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア秘密鍵を用いて前記暗号化情報固有鍵を復号して情報固有鍵を取り出し、この情報固有鍵を用いて前記暗号化情報を復号して目的情報を取り出すことを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送、記録および利用方法。

【請求項 5】 サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報が既に情報記録装置の記憶メディア内に記憶されており、サーバの記憶装置に蓄積されている情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、

サーバにおいて前記メディア公開鍵で前記情報固有鍵を暗号化して暗号化情報固有鍵を生成し、

前記暗号化情報固有鍵を情報記録装置に送信し、情報記録装置は前記暗号化情報固有鍵を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。

【請求項 6】 書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、

情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第 1 の暗号情報 K 1 を生成し、

鍵サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第 1 の暗号情報 K 1 を暗号化して第 2 の暗号情報 K 2 を生成し、

不正利用を防止したい目的情報に対して情報固有鍵を生成し、この情報固有鍵を用いて前記目的情報を暗号化し

た暗号化情報を生成し、

前記情報固有鍵を前記第 1 の暗号情報 K 1 で暗号化して K 1 暗号化情報固有鍵を生成し、

前記暗号化情報と前記 K 1 暗号化情報固有鍵を記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報記録方法。

【請求項 7】 書換え不可能な独自の識別子を有する記憶メディアに記録された情報の利用を行う情報利用方法であって、

情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第 1 の暗号情報 K 1 を生成し、

前記情報固有鍵を前記第 1 の暗号情報 K 1 で暗号化して K 1 暗号化情報固有鍵を生成し、

不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と前記情報固有鍵を前記第 1 の暗号情報 K 1 で暗号化した K 1 暗号化情報固有鍵が記録されている記憶メディアから前記 K 1 暗号化情報固有鍵を読み出し、

この読み出した K 1 暗号化情報固有鍵を前記第 1 の暗号情報 K 1 で復号して、情報固有鍵を取り出し、

前記暗号化情報を前記記憶メディアから読み出し、この暗号化情報を前記情報固有鍵で復号して前記目的情報を取り出して利用することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報利用方法。

【請求項 8】 サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と情報固有鍵をサーバ記憶装置に蓄積し、この蓄積されている暗号化情報と情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、

情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第 1 の暗号情報 K 1 を生成し、

サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第 1 の暗号情報 K 1 を暗号化して第 2 の暗号情報 K 2 を生成し、この第 2 の暗号情報 K 2 をサーバに送信し、

サーバにおいて前記第 2 の暗号情報 K 2 を前記配送用共通鍵で復号して前記第 1 の暗号情報 K 1 を生成し、

この第 1 の暗号情報 K 1 で前記情報固有鍵を暗号化して K 1 暗号化情報固有鍵を生成し、

前記 K 1 暗号化情報固有鍵と前記暗号化情報を情報記録装置に送信し、

情報記録装置は前記 K 1 暗号化情報固有鍵と前記暗号化情報を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。

【請求項 9】 サーバにおいて不正利用を防止したい目

的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報が既に情報記録装置の記憶メディア内に記憶されており、サーバの記憶装置に蓄積されている情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、

情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第 1 の暗号情報 K 1 を生成し、

サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第 1 の暗号情報 K 1 を暗号化して第 2 の暗号情報 K 2 を生成し、この第 2 の暗号情報 K 2 をサーバに送信し、

サーバにおいて前記第 2 の暗号情報 K 2 を前記配送用共通鍵で復号して前記第 1 の暗号情報 K 1 を生成し、

この第 1 の暗号情報 K 1 で前記情報固有鍵を暗号化して K 1 暗号化情報固有鍵を生成し、

前記 K 1 暗号化情報固有鍵を情報記録装置に送信し、

情報記録装置は前記 K 1 暗号化情報固有鍵を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。

【請求項 10】 書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、

このメディア公開鍵を用いて暗号化した目的情報を記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報記録方法。

【請求項 11】 書換え不可能な独自の識別子を有する記憶メディアに記録されている暗号化情報を利用する情報利用方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、

前記記憶メディアに記録されている暗号化情報を読み出し、この暗号化情報を前記メディア秘密鍵で復号して、

目的情報を取り出して利用することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報利用方法。

【請求項 12】 サーバに蓄積されている目的情報を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、

サーバにおいて前記メディア公開鍵で前記目的情報を暗

号化して暗号化情報を生成し、

サーバは前記暗号化情報を情報記録装置に送信し、

情報記録装置は前記暗号化情報を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、不正利用を防止したい電子情報である目的情報を暗号化して情報提供側からの情報記録利用側に配送し、この配送された目的情報を書換え不可能な独自の識別子（以下、IDと略称する）を有する記憶メディアに記録し、この記録された目的情報を利用する記憶メディア識別子を利用した不正利用防止のための情報記録、利用および配送方法に関する。

【0002】

【従来の技術】電子情報は容易に複製可能であるという性質を持っている。一方、情報の提供者は情報に付加価値を付け、情報を販売したい場合がある。このように情報を販売する場合、情報の利用者によって情報が他のメディアに複製され、対価を払って情報を購入した正規の利用者以外に情報が利用されてしまうことがある。

【0003】盗聴や不正利用を避けるために、情報を暗号化して配送および保存する方法が容易に考えられるが、情報を利用する際に情報を復号化するための復号鍵が必要になる。しかし、この方法では、暗号化した情報と復号鍵の両情報を複製された場合に、容易に不正利用が可能である。

【0004】更に、これを避けるために、復号鍵を複製できない装置内に保存する場合、情報を利用するためには、復号鍵を保存した装置が必要になり、可搬性が悪くなるという問題がある。

【0005】また、情報を販売する場合、利用者が対価を払って情報を購入する際に、情報は提供者から利用者の装置へ配送される。この配送の途中において盗聴をされた場合、盗聴した情報から元の情報が容易に再現され、対価を払って情報を購入していない盗聴者に情報が利用されてしまうことがある。

【0006】

【発明が解決しようとする課題】上述したように、情報の提供者が販売した情報は、不正に複製された場合に、容易に不正利用されてしまうという問題がある。また、暗号化して情報を配布したとしても、暗号化した情報と、暗号化した情報を復号するための復号鍵を共に複製された場合、これも容易に不正利用されてしまうという問題がある。

【0007】また、復号鍵の複製を避けるために、復号鍵を複製できない装置内に保存する場合、情報の可搬性が下がるという問題がある。

【0008】更に、情報を販売する際の配送経路におい

ても、情報が盗聴された場合に不正利用されてしまうという問題がある。

【0009】本発明は、上記に鑑みてなされたもので、その目的とするところは、記憶メディア独自の書換え不可能な識別子を利用することにより他の記憶メディアに複製しても利用できないようにした記憶メディア識別子を利用した不正利用防止のための情報記録、利用および配送方法を提供することにある。

【0010】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、不正利用を防止したい目的情報に対して情報固有鍵を生成し、この情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、前記情報固有鍵を前記メディア公開鍵で暗号化した暗号化情報固有鍵を生成し、前記暗号化情報と前記暗号化情報固有鍵を記憶メディアに記録することを要旨とする。

【0011】請求項1記載の本発明にあつては、暗号化情報固有鍵から情報固有鍵を復号するにはメディア秘密鍵が必要であるが、このメディア秘密鍵は記憶メディア独自の識別子から生成されるため、記憶メディアに記録されている暗号化情報固有鍵、暗号化情報、鍵対応情報を読み出して別の記憶メディアに複製しても、この別の記憶メディアの独自の識別子から生成されるメディア秘密鍵では暗号化情報固有鍵を復号できず、従って情報の複製による不正利用を防止することができる。

【0012】また、請求項2記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアに記録された情報の利用を行う情報利用方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と前記情報固有鍵を前記メディア公開鍵で暗号化した暗号化情報固有鍵を記録している前記記憶メディアから前記暗号化情報固有鍵を読み出し、この読み出した暗号化情報固有鍵を前記メディア秘密鍵で復号して、情報固有鍵を取り出し、前記暗号化情報を前記記憶メディアから読み出し、この暗号化情報を前記情報固有鍵で復号して前記目的情報を取り出して利用することを要旨とする。

【0013】請求項2記載の本発明にあつては、記憶メディアから読み出した暗号化情報固有鍵を記憶メディアの識別子から生成したメディア秘密鍵で復号して、情報固有鍵を取り出し、情報固有鍵で暗号化情報を復号して目的情報を取り出すため、記憶メディアに記録されている暗号化情報固有鍵、暗号化情報、鍵対応情報を読み出して別の記憶メディアに複製しても、この別の記憶メデ

ィアの独自の識別子から生成されるメディア秘密鍵では暗号化情報固有鍵を復号できず、従って情報の複製による不正利用を防止することができる。

【0014】更に、請求項3記載の本発明は、サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と情報固有鍵をサーバ記憶装置に蓄積し、この蓄積されている暗号化情報と情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、サーバにおいて前記メディア公開鍵で前記情報固有鍵を暗号化して暗号化情報固有鍵を生成し、前記暗号化情報固有鍵と前記暗号化情報を情報記録装置に送信し、情報記録装置は前記暗号化情報固有鍵と前記暗号化情報を受信して、記憶メディアに記録することを要旨とする。

【0015】請求項3記載の本発明にあつては、情報記録装置からサーバに送信される記憶メディアの情報はメディア公開鍵のみであり、通信中に盗聴されても不正利用はできず、またサーバから情報記録装置に送信される情報は暗号化情報固有鍵と暗号化情報であり、暗号化情報固有鍵は記憶メディアの識別子から生成したメディア秘密鍵がなければ情報固有鍵に復号できず、この情報固有鍵がなければ暗号化情報から目的情報を復号できない。従って、暗号化情報固有鍵と暗号化情報は通信中に盗聴されても不正利用することはできない。

【0016】請求項4記載の本発明は、情報提供側からの目的情報を情報利用側に配送し、書換え不可能な独自の識別子を有する記憶メディアに目的情報を記録し、この記録された目的情報を利用する情報の配送、記録および利用方法であって、情報提供側において、前記目的情報に対して情報固有鍵を生成し、この生成した情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、この暗号化情報と前記情報固有鍵を記憶しておき、情報利用側において、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵を情報提供側に配送し、情報提供側において、前記メディア公開鍵を受信し、このメディア公開鍵で前記情報固有鍵を暗号化した暗号化情報固有鍵を生成し、この生成した暗号化情報固有鍵と前記暗号化情報を情報利用側に配送し、情報利用側において、前記暗号化情報固有鍵と前記暗号化情報を受信し、この受信した暗号化情報固有鍵と暗号化情報を前記記憶メディアに記録し、情報利用側において、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア秘密鍵を用いて前記暗号化情報固有鍵を復号して情報固有鍵を取り出し、この情報固有鍵を用いて前記暗号化情報を復号して

目的情報を取り出すことを要旨とする。

【0017】請求項4記載の本発明にあつては、情報提供側において目的情報から生成される情報固有鍵を用いて目的情報を暗号化した暗号化情報を生成し、この暗号化情報と情報固有鍵を記憶しておき、情報利用側において記憶メディアの識別子を利用してメディア公開鍵とメディア秘密鍵を生成し、該メディア公開鍵を情報提供側に配送し、情報提供側において受信したメディア公開鍵で情報固有鍵を暗号化した暗号化情報固有鍵と暗号化情報を情報利用側に配送し、情報利用側において受信した暗号化情報固有鍵と暗号化情報を記憶メディアに記録し、情報利用側においてメディア秘密鍵を用いて暗号化情報固有鍵を復号して情報固有鍵を取り出し、この情報固有鍵を用いて暗号化情報を復号して目的情報を取り出すため、暗号化情報固有鍵、暗号化情報を記憶メディアから読み出して別の記憶メディアに複製しても、この別の記憶メディアの独自の識別子から生成されるメディア秘密鍵では暗号化情報固有鍵を復号できず、従って情報の複製による不正利用を防止することができるとともに、暗号化情報固有鍵は記憶メディアの識別子から生成したメディア秘密鍵がなければ情報固有鍵に復号できず、この情報固有鍵がなければ暗号化情報から目的情報を復号できないため、暗号化情報固有鍵と暗号化情報は通信中に盗聴されても不正利用することはできない。

【0018】また、請求項5記載の本発明は、サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報が既に情報記録装置の記憶メディア内に記憶されており、サーバの記憶装置に蓄積されている情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、サーバにおいて前記メディア公開鍵で前記情報固有鍵を暗号化して暗号化情報固有鍵を生成し、前記暗号化情報固有鍵を情報記録装置に送信し、情報記録装置は前記暗号化情報固有鍵を受信して、記憶メディアに記録することを要旨とする。

【0019】請求項5記載の本発明にあつては、情報記録装置からサーバに送信される記憶メディアの情報はメディア公開鍵のみであり、通信中に盗聴されても不正利用はできず、またサーバから情報記録装置に送信される情報は暗号化情報固有鍵のみであり、暗号化情報固有鍵は記憶メディアの識別子から生成したメディア秘密鍵がなければ情報固有鍵に復号できず、従って暗号化情報固有鍵が通信中に盗聴されても不正利用することはできない。

【0020】更に、請求項6記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、情報記録装置と情

報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第1の暗号情報K1を生成し、鍵サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第1の暗号情報K1を暗号化して第2の暗号情報K2を生成し、不正利用を防止したい目的情報に対して情報固有鍵を生成し、この情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、前記情報固有鍵を前記第1の暗号情報K1で暗号化してK1暗号化情報固有鍵を生成し、前記暗号化情報と前記K1暗号化情報固有鍵を記憶メディアに記録することを要旨とする。

【0021】請求項6記載の本発明にあっては、K1暗号化情報固有鍵から情報固有鍵を復号するには、第1の暗号情報K1が必要であり、この第1の暗号情報K1は記憶メディア独自の識別子から利用共通鍵を用いて生成されるため、記憶メディアから暗号化情報、K1暗号化情報固有鍵を別の記憶メディアに複製しても、別の記憶メディアの独自の識別子から生成される第1の暗号情報K1では復号できず、従って情報の複製による不正利用を防止することができる。

【0022】請求項7記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアに記録された情報の利用を行う情報利用方法であって、情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第1の暗号情報K1を生成し、前記情報固有鍵を前記第1の暗号情報K1で暗号化してK1暗号化情報固有鍵を生成し、不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と前記情報固有鍵を前記第1の暗号情報K1で暗号化したK1暗号化情報固有鍵が記録されている記憶メディアから前記K1暗号化情報固有鍵を読み出し、この読み出したK1暗号化情報固有鍵を前記第1の暗号情報K1で復号して、情報固有鍵を取り出し、前記暗号化情報を前記記憶メディアから読み出し、この暗号化情報を前記情報固有鍵で復号して前記目的情報を取り出して利用することを要旨とする。

【0023】請求項7記載の本発明にあっては、記憶メディアから読み出したK1暗号化情報固有鍵を記憶メディアの識別子から生成した第1の暗号情報K1で復号して、情報固有鍵を取り出し、情報固有鍵で暗号化情報を復号して目的情報を取り出すため、記憶メディアに記録されているK1暗号化情報固有鍵、暗号化情報を読み出して別の記憶メディアに複製しても、別の記憶メディアの独自の識別子から生成される第1の暗号情報K1ではK1暗号化情報固有鍵を復号できず、従って情報の複製による不正利用を防止することができる。

【0024】また、請求項8記載の本発明は、サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報

と情報固有鍵をサーバ記憶装置に蓄積し、この蓄積されている暗号化情報と情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第1の暗号情報K1を生成し、サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第1の暗号情報K1を暗号化して第2の暗号情報K2を生成し、この第2の暗号情報K2をサーバに送信し、サーバにおいて前記第2の暗号情報K2を前記配送用共通鍵で復号して前記第1の暗号情報K1を生成し、この第1の暗号情報K1で前記情報固有鍵を暗号化してK1暗号化情報固有鍵を生成し、前記K1暗号化情報固有鍵と前記暗号化情報を情報記録装置に送信し、情報記録装置は前記K1暗号化情報固有鍵と前記暗号化情報を受信して、記憶メディアに記録することを要旨とする。

【0025】請求項8記載の本発明にあっては、情報記録装置からサーバに送信される記憶メディアの情報は第2の暗号情報K2のみであり、第2の暗号情報K2が通信中に盗聴されても配送用共通鍵が知られない限り不正利用はできず、またサーバから情報記録装置に送信される情報はK1暗号化情報固有鍵と暗号化情報であり、K1暗号化情報固有鍵は利用サーバ鍵と記憶メディア独自の識別子がなければ情報固有鍵に復号できず、暗号化情報は情報固有鍵がなければ目的情報に復号できない。従って、K1暗号化情報固有鍵と暗号化情報は通信中に盗聴されても不正利用できない。

【0026】更に、請求項9記載の本発明は、サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報が既に情報記録装置の記憶メディア内に記憶されており、サーバの記憶装置に蓄積されている情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第1の暗号情報K1を生成し、サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第1の暗号情報K1を暗号化して第2の暗号情報K2を生成し、この第2の暗号情報K2をサーバに送信し、サーバにおいて前記第2の暗号情報K2を前記配送用共通鍵で復号して前記第1の暗号情報K1を生成し、この第1の暗号情報K1で前記情報固有鍵を暗号化してK1暗号化情報固有鍵を生成し、前記K1暗号化情報固有鍵を情報記録装置に送信し、情報記録装置は前記K1暗号化情報

報固有鍵を受信して、記憶メディアに記録することを要旨とする。

【0027】請求項9記載の本発明にあつては、情報記録装置からサーバに送信される記憶メディアの情報は第2の暗号情報K2のみであり、この第2の暗号情報K2が通信中に盗聴されても配送用サーバ鍵が知られない限り不正利用はできず、またサーバから情報記録装置に送信される情報はK1暗号化情報固有鍵のみであり、K1暗号化情報固有鍵は利用サーバ鍵と記憶メディア独自の識別子がなければ情報固有鍵に復号できず、従つてK1暗号化情報固有鍵は通信中に盗聴されても不正利用できない。

【0028】請求項10記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であつて、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵を用いて暗号化した目的情報を記憶メディアに記録することを要旨とする。

【0029】請求項10記載の本発明にあつては、暗号化情報を復号するにはメディア秘密鍵が必要であり、メディア秘密鍵は記憶メディア独自の識別子から生成されるため、記憶メディアから暗号化情報が別の記憶メディアに複製されても、別の記憶メディア独自の識別子から生成されるメディア秘密鍵では暗号化情報を復号できず、従つて情報の複製による不正利用を防止することができる。

【0030】また、請求項11記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアに記録されている暗号化情報を利用する情報利用方法であつて、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、前記記憶メディアに記録されている暗号化情報を読み出し、この暗号化情報を前記メディア秘密鍵で復号して、目的情報を取り出して利用することを要旨とする。

【0031】請求項11記載の本発明にあつては、記憶メディアから読み出した暗号化情報を記憶メディアの識別子から生成したメディア秘密鍵で復号して目的情報を取り出すため、記憶メディアに記録されている暗号化情報を読み出して別の記憶メディアに複製しても、別の記憶メディアの独自の識別子から生成されるメディア秘密鍵では暗号化情報を復号できず、従つて情報の複製による不正利用を防止することができる。

【0032】更に、請求項12記載の本発明は、サーバに蓄積されている目的情報を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であつて、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、サーバにおいて前記メディア公開鍵で前記目的

情報を暗号化して暗号化情報を生成し、サーバは前記暗号化情報を情報記録装置に送信し、情報記録装置は前記暗号化情報を受信して、記憶メディアに記録することを要旨とする。

【0033】請求項12記載の本発明にあつては、情報記録装置からサーバに送信される情報はメディア公開鍵のみであり、メディア公開鍵は記憶メディア独自の識別子から生成されるものであるため、通信中に盗聴されても不正利用できない。また、サーバから情報記録装置に送信される目的情報はメディア公開鍵で暗号化されており、通信中に盗聴されても不正利用できない。

【0034】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図1は、本発明の第1の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。図1に示す実施形態1のシステムは、記憶メディア1と、この記憶メディア1に情報を書き込む情報記録装置2と、記憶メディア1に格納された情報を利用する際に使う情報利用装置3と、情報を配信する鍵サーバ4から構成され、元の目的情報は情報提供者5から提供される。

【0035】記憶メディア1は記憶メディア独自のID(識別子)11と、通常書換え可能な記憶領域12から構成される。

【0036】また記憶メディア1に情報を書き込む情報記録装置2は、公開鍵ペア生成処理部21と情報記録処理部22を持っており、記憶メディア1を装着した上で記憶メディア1からの記憶メディア独自のID11の読み出しと、記憶領域12への書き込みを行うことができる。

【0037】情報を配信する鍵サーバ4は、メディア公開鍵を用いて情報固有鍵を暗号化した暗号化情報固有鍵を作成するための公開鍵暗号化処理部41と、暗号化情報および情報固有鍵を蓄積する記憶装置42と、情報暗号化処理部43からなる。

【0038】情報提供者5は予め目的情報Cを鍵サーバ4に送信し、鍵サーバ4内の情報暗号化処理部43にて情報固有鍵Kcとこの情報固有鍵Kcで暗号化した暗号情報Ec(Kc, C)を作成しておき、情報固有鍵Kcと暗号情報Ec(Kc, C)を鍵サーバ4内の記憶装置42に記録しておく。

【0039】目的情報を鍵サーバ4から記憶メディア1まで配送する場合には、まず、記憶メディア1から記憶メディア独自のID11を読み出し、情報記録装置2内部の公開鍵ペア生成処理部21で、記憶メディア独自のID11を利用してメディア公開鍵Kpmとメディア秘密鍵Ksmを生成し、メディア公開鍵Kpmを鍵サーバ4に送信する。メディア公開鍵Kpmを受信した鍵サーバ4では、記憶装置42から情報固有鍵Kcを取り出

し、公開鍵暗号化処理部 41 で、情報固有鍵 Kc をメディア公開鍵 Kpm を用いて暗号化し、暗号化情報固有鍵 Ep (Kpm, Kc) を生成する。

【0040】次いで、鍵サーバ 4 は暗号情報 Ec (Kc, C) と暗号化情報固有鍵 Ep (Kpm, Kc) を情報記録装置 2 へ送信する。暗号情報 Ec (Kc, C) と暗号化情報固有鍵 Ep (Kpm, Kc) を受け取った情報記録装置 2 では、情報記録処理部 22 にて記憶メディア 1 の記憶領域 12 へ暗号情報 Ec (Kc, C) と暗号化情報固有鍵 Ep (Kpm, Kc) を記録する。

【0041】この配送方法を利用して配送経路上の盗聴の脅威を考えた場合、配送経路上を流れるデータはメディア公開鍵 Kpm と暗号情報 Ec (Kc, C) と暗号化情報固有鍵 Ep (Kpm, Kc) であり、メディア秘密鍵 Ksm がなければ暗号化情報固有鍵 Ep (Kpm, Kc) は復号できず、情報固有鍵 Kc がなければ暗号情報 Ec (Kc, C) は復号できず、メディア公開鍵 Kpm は盗聴されても問題がないために、配送経路上を流れるデータを盗聴されても目的情報 C を復元することができないため、安全である。

【0042】次に、上記実施形態 1 で記憶メディア 1 に記録された情報を利用する方法について述べる。情報利用装置 3 は公開鍵ペア生成処理部 31 と鍵復号処理部 32 と情報復号処理部 33 と情報利用処理部 34 を持ち、記憶メディア 1 を装着した上で記憶メディア 1 からの記憶メディア独自の ID11 の読み出しと、記憶領域 12 からの読み出しを行うことができる。なお、公開鍵ペア生成処理部 31 は情報記録装置 2 の公開鍵ペア生成処理部 21 と同じアルゴリズムを用いて公開鍵および暗号鍵

の生成を行うものとする。

【0043】情報の配送後、情報を利用する場合、記憶メディア 1 は情報記録装置 2 から取り出され、情報利用装置 3 に装着されているものとする。

【0044】情報を利用する際に、まず記憶メディア 1 から記憶メディア独自の ID11 を読み出し、情報利用装置 3 内部の公開鍵ペア生成処理部 31 で、記憶メディア独自の ID11 を利用してメディア公開鍵 Kpm とメディア秘密鍵 Ksm を生成し、鍵復号処理部 32 にメディア秘密鍵 Ksm を渡し、鍵復号処理部 32 は記憶メディア 1 の記憶領域 12 から暗号化情報固有鍵 Ep (Kpm, Kc) を読み出し、暗号化情報固有鍵 Ep (Kpm, Kc) をメディア秘密鍵 Ksm で復号し情報固有鍵 Kc を得て、情報復号処理部 33 に渡し、情報復号処理部 33 は記憶メディア 1 の記憶領域 12 から暗号情報 Ec (Kc, C) を読み出し、暗号情報 Ec (Kc, C) を情報固有鍵 Kc で復号し目的情報 C を得て、情報利用処理部 34 へ渡す。情報利用処理部 34 は、目的情報 C を利用するための処理を行うものとし、ここではその処理を規定しないが、音楽、動画像、静止画像、テキスト等の各種情報の再生等が考えられる。

【0045】ここで不正利用者が、記憶メディア 1 から暗号情報 Ec (Kc, C) と暗号化情報固有鍵 Ep (Kpm, Kc) を読み出し、別の記憶メディアに複製した場合を考える。このとき、別の記憶メディアには記憶メディア独自の ID があるが、これは書換えができないため複製することができない。複製した記憶メディアを用いて上記情報利用装置で情報を利用しようとした場合、公開鍵ペア生成処理部 31 では、メディア公開鍵 Kpm' とメディア秘密鍵 Ksm' が生成されるが、このメディア秘密鍵 Ksm' では暗号化情報固有鍵 Ep (Kpm, Kc) から情報固有鍵 Kc を復号することはできない。このため、暗号情報 Ec (Kc, C) から目的情報 C を復号することもできず、結局複製した記憶メディアでは目的情報を利用することはできないため、情報は不正利用できない。一方、正当な利用者は記憶メディア 1 を、情報利用装置 3 の機能を備えた任意の装置に装着することで情報の利用が可能であり、可搬性を保つことができる。

【0046】図 2 は、本発明の第 2 の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。同図に示す実施形態 2 のシステムは、目的情報を情報固有鍵で暗号化した暗号化情報を情報提供者 5 において CD-ROM 等 6 やインターネット等の経路を通じて予め利用者に配送し、記憶メディア 1 の記憶領域 12 に既に格納されている点が図 1 に示した実施形態 1 と異なるものである。

【0047】すなわち、図 2 に示す実施形態 2 のシステムは、記憶メディア 1 と、記憶メディアに情報を書き込む情報記録装置 2 と、記憶メディア 1 に格納された情報を利用する際に使う情報利用装置 3 と、情報を配信する鍵サーバ 4 から構成され、元の目的情報は情報提供者 5 から提供される。

【0048】記憶メディア 1 は記憶メディア独自の ID11 と、通常書換え可能な記憶領域 12 から構成される。

【0049】また、記憶メディア 1 に情報を書き込む情報記録装置 2 は、公開鍵ペア生成処理部 21 と情報記録処理部 22 を持っており、記憶メディア 1 を装着した上で記憶メディア 1 からの記憶メディア独自の ID11 の読み出しと、記憶領域 12 への書き込みを行うことができる。

【0050】鍵情報を配信する鍵サーバ 4 は、メディア公開鍵を用いて情報固有鍵を暗号化した暗号化情報固有鍵を作成するための公開鍵暗号化処理部 41 と、暗号化情報および情報固有鍵を蓄積する記憶装置 42 と、情報暗号化処理部 43 からなる。

【0051】情報提供者は予め目的情報 C を鍵サーバ 4 に送信し、鍵サーバ 4 内の情報暗号化処理部 43 にて情報固有鍵 Kc とこの情報固有鍵 Kc で目的情報を暗号化

した暗号情報 E c (K c , C) を作成して、情報固有鍵 K c を鍵サーバ 4 内の記憶装置 4 2 に記録しておき、暗号情報 E c (K c , C) は情報提供者が C D - R O M やインターネット等の経路を通じて予め利用者まで情報を配送しており、暗号情報 E c (K c , C) は既に記憶メディア 1 の記憶領域 1 2 内に格納されているものとする。

【 0 0 5 2 】 情報固有鍵 K c を鍵サーバ 4 から記憶メディア 1 まで配送する場合には、まず、記憶メディア 1 から記憶メディア独自の I D 1 1 を読み出し、情報記録装置 2 内部の公開鍵ペア生成処理部 2 1 で、メディア公開鍵 K p m とメディア秘密鍵 K s m を生成し、メディア公開鍵 K p m を鍵サーバ 4 に送信する。メディア公開鍵 K p m を受信した鍵サーバ 4 では、記憶装置 4 2 から情報固有鍵 K c を取り出し、公開鍵暗号化処理部 4 1 で、情報固有鍵 K c をメディア公開鍵 K p m を用いて暗号化し、暗号化情報固有鍵 E p (K p m , K c) を生成する。

【 0 0 5 3 】 次いで、鍵サーバ 4 は暗号化情報固有鍵 E p (K p m , K c) を情報記録装置 2 へ送信する。暗号化情報固有鍵 E p (K p m , K c) を受け取った情報記録装置 2 では、情報記録処理部 2 2 にて記憶メディア 1 の記憶領域 1 2 へ、暗号化情報固有鍵 E p (K p m , K c) を記録する。この配送方法において配送経路上の盗聴の脅威を考えた場合、配送経路上を流れるデータはメディア公開鍵 K p m と暗号化情報固有鍵 E p (K p m , K c) であり、メディア秘密鍵 K s m がなければ暗号化情報固有鍵 E p (K p m , K c) は復号できず、例えば盗聴者が暗号情報 E c (K c , C) を入手していたとしても情報固有鍵 K c がなければ暗号情報 E c (K c , C) は復号できず、メディア公開鍵 K p m は盗聴されても問題がないために、配送経路上を流れるデータを盗聴されても目的情報 C を復元することができないため、安全である。

【 0 0 5 4 】 また、実施形態 2 の方法で記憶メディア 1 に記録された情報を利用する場合の方法については、実施形態 1 の情報利用方法と同じであるため、省略する。実施形態 2 の場合、目的情報 C が大容量の場合でも鍵サーバ 4 と情報記録装置 2 の間の通信量は大きくならないため利用者の負担を減らすことができる。

【 0 0 5 5 】 図 3 は、本発明の第 3 の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。同図に示す実施形態 3 のシステムは、記憶メディア 1 と、記憶メディアに情報を書き込む情報記録装置 7 と、記憶メディア 1 に格納された情報を利用する際に使う情報利用装置 8 と、情報を配信する鍵サーバ 9 から構成され、元の目的情報は情報提供者 5 から提供される。

【 0 0 5 6 】 記憶メディア 1 は記憶メディア独自の I D

1 1 と、通常の手換え可能な記憶領域 1 2 から構成される。

【 0 0 5 7 】 また、記憶メディア 1 に情報を書き込む情報記録装置 7 は、K 1 生成処理部 7 1 と K 2 生成処理部 7 2 と情報記録処理部 7 3 を持っており、記憶メディア 1 を装着した上で記憶メディア 1 からの記憶メディア独自の I D 1 1 の読み出しと、記憶領域 1 2 への書き込みを行うことができる。

【 0 0 5 8 】 情報を配信する鍵サーバ 9 は、配送用共通鍵を用いて K 2 から K 1 を復号する K 2 復号化処理部 9 1 と、K 1 を用いて情報固有鍵を暗号化した K 1 暗号化情報固有鍵を作成するための鍵暗号化処理部 9 2 と、暗号化情報および情報固有鍵を蓄積する記憶装置 9 3 と、情報暗号化処理部 9 4 からなる。

【 0 0 5 9 】 情報提供者は予め目的情報 C を鍵サーバ 9 に送信し、鍵サーバ 9 内の情報暗号化処理部 9 4 にて情報固有鍵 K c と暗号情報 E c (K c , C) を作成しておき、情報固有鍵 K c と暗号情報 E c (K c , C) は鍵サーバ 9 内の記憶装置 9 3 に記録しておく。

【 0 0 6 0 】 目的情報を鍵サーバ 9 から記憶メディア 1 まで配送する場合には、まず、記憶メディア 1 から記憶メディア独自の I D 1 1 を読み出し、この記憶メディア独自の I D 1 1 から情報記録装置 7 内部の K 1 生成処理部 7 1 で利用共通鍵を用いて K 1 を生成し、次のその K 1 から情報記録装置 7 内部の K 2 生成処理部 7 2 で配送用共通鍵を用いて K 2 を生成し、K 2 を鍵サーバ 9 に送信する。K 2 を受信した鍵サーバ 9 では、まず K 2 復号化処理部で配送用共通鍵を用いて K 2 から K 1 を復号し、記憶装置 9 3 から情報固有鍵 K c を取り出し、鍵暗号化処理部 9 2 で、情報固有鍵 K c を K 1 を用いて暗号化し、K 1 暗号化情報固有鍵 E c (K 1 , K c) を生成する。

【 0 0 6 1 】 次いで、鍵サーバ 9 は暗号情報 E c (K c , C) と K 1 暗号化情報固有鍵 E c (K 1 , K c) を情報記録装置 7 へ送信する。暗号情報 E c (K c , C) と K 1 暗号化情報固有鍵 E c (K 1 , K c) を受け取った情報記録装置 7 では、情報記録処理部 7 3 にて記憶メディア 1 の記憶領域 1 2 へ、暗号情報 E c (K c , C) と K 1 暗号化情報固有鍵 E c (K 1 , K c) を記録する。

【 0 0 6 2 】 この配送方法を利用して配送経路上の盗聴の脅威を考えた場合、配送経路上を流れるデータは K 2 と暗号情報 E c (K c , C) と K 1 暗号化情報固有鍵 E c (K 1 , K c) であり、配送用共通鍵を知らなければ K 2 から K 1 を求めることはできず、K 1 がなければ K 1 暗号化情報固有鍵 E c (K 1 , K c) から情報固有鍵 K c は復号できず、情報固有鍵 K c がなければ暗号情報 E c (K c , C) は復号できないため、配送経路上を流れるデータを盗聴されても目的情報 C を復元することができないため、安全である。

【0063】次に、上記実施形態3で記憶メディア1に記録された情報を利用する方法について述べる。情報利用装置8はK1生成処理部81と鍵復号処理部82と情報復号処理部83と情報利用処理部84を持ち、記憶メディア1を装着した上で記憶メディア1からの記憶メディア独自のID11の読み出しと、記憶領域12からの読み出しを行うことができる。なお、K1生成処理部81は情報記録装置7のK1生成処理部71と同じアルゴリズムを用い、またK1生成の際に用いる利用共通鍵を情報記録装置7のK1生成処理部71と共有しているものとする。

【0064】情報の配送後、情報を利用する場合、記憶メディア1は情報記録装置7から取り出し、情報利用装置8に装着されているものとする。

【0065】情報を利用する際に、まず記憶メディア1から記憶メディア独自のID11を読み出し、この記憶メディア独自のID11から情報利用装置8内部のK1生成処理部81で利用共通鍵を用いてK1を生成し、鍵復号処理部82にK1を渡し、鍵復号処理部82は記憶メディア1の記憶領域12からK1暗号化情報固有鍵Ec(K1, Kc)を読み出し、K1暗号化情報固有鍵Ec(K1, Kc)をK1で復号し情報固有鍵Kcを得て、情報復号処理部83に渡し、情報復号処理部83は記憶メディア1の記憶領域12から暗号情報Ec(Kc, C)を読み出し、暗号情報Ec(Kc, C)を情報固有鍵Kcで復号し目的情報Cを得て、情報利用処理部84を渡す。情報利用処理部84は、目的情報Cを利用するための処理を行うものとし、ここではその処理を規定しないが、音楽、動画像、静止画像、テキスト等の各種情報の再生などが考えられる。

【0066】ここで不正利用者が、記憶メディア1から暗号情報Ec(Kc, C)とK1暗号化情報固有鍵Ec(K1, Kc)を読み出し、別の記憶メディアに複製した場合を考える。このとき、別の記憶メディアには記憶メディア独自のIDがあるが、これは書換えができないため複製することができない。複製した記憶メディアを用いて上記情報利用装置で情報を利用しようとした場合、K1生成処理部31では、K1'が生成されるが、このK1'ではK1暗号化情報固有鍵Ec(K1, Kc)から情報固有鍵Kcを復号することはできない。このため、暗号情報Ec(Kc, C)から目的情報Cを復号することもできず、結局複製した記憶メディアでは目的情報を利用することはできないため、情報は不正利用できない。一方、正当な利用者は記憶メディア1を、情報利用装置3の機能を備えた任意の装置に装着することで情報の利用が可能であり、可搬性を保つことができる。

【0067】図4は、本発明の第4の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を

示すブロック図である。同図に示す実施形態4のシステムは、目的情報を情報固有鍵で暗号化した暗号化情報を情報提供者5においてCD-ROM等6やインターネット等の経路を通じて予め利用者に配送し、記憶メディア1の記憶領域12に既に格納されている点が図3に示した実施形態3と異なるものである。

【0068】すなわち、図4に示す実施形態4のシステムは、記憶メディア1と、記憶メディアに情報を書き込む情報記録装置7と、記憶メディア1に格納された情報を利用する際に使う情報利用装置8と、情報を配信する鍵サーバ9から構成され、元の目的情報は情報提供者5から提供される。

【0069】記憶メディア1は記憶メディア独自のID11と、通常の書換え可能な記憶領域12から構成される。

【0070】また、記憶メディア1に情報を書き込む情報記録装置7は、K1生成処理部71とK2生成処理部72と情報記録処理部73を持っており、記憶メディア1を装着した上で記憶メディア1からの記憶メディア独自のID11の読み出しと、記憶領域12への書き込みを行うことができる。

【0071】情報を配信する鍵サーバ9は、配送用共通鍵を用いてK2からK1を復号するK2復号化処理部91と、K1を用いて情報固有鍵を暗号化したK1暗号化情報固有鍵を作成するための鍵暗号化処理部92と、暗号化情報および情報固有鍵を蓄積する記憶装置93と、情報暗号化処理部94からなる。

【0072】情報提供者は予め目的情報Cを鍵サーバ9に送信し、鍵サーバ9内の情報暗号化処理部94にて情報固有鍵Kcとこの情報固有鍵Kcで目的情報Cを暗号化した暗号情報Ec(Kc, C)を作成し、情報固有鍵Kcは鍵サーバ9内の記憶装置93に記録しておき、暗号情報Ec(Kc, C)は情報提供者がCD-ROMやインターネット等の経路を通じて予め利用者まで情報を配送しており、暗号情報Ec(Kc, C)は既に記憶メディア1の記憶領域12内に格納されているものとする。

【0073】情報固有鍵Kcを鍵サーバ9から記憶メディア1まで配送する場合には、まず、記憶メディア1から記憶メディア独自のID11を読み出し、情報記録装置7内部のK1生成処理部71で利用共通鍵を用いてK1を生成し、次にそのK1から情報記録装置7内部のK2生成処理部72で配送用共通鍵を用いてK2を生成し、K2を鍵サーバ9に送信する。K2を受信した鍵サーバ9では、まずK2復号化処理部で配送用共通鍵を用いてK2からK1を復号し、記憶装置93から情報固有鍵Kcを取り出し、鍵暗号化処理部92で、情報固有鍵KcをK1を用いて暗号化し、K1暗号化情報固有鍵Ec(K1, Kc)を生成する。

【0074】次いで、鍵サーバ9はK1暗号化情報固有

鍵Ec (K1, Kc) を情報記録装置7へ送信する。K1暗号化情報固有鍵Ec (K1, Kc) を受け取った情報記録装置7では、情報記録処理部73にて記憶メディア1の記憶領域12に暗号情報Ec (Kc, C) とK1暗号化情報固有鍵Ec (K1, Kc) を記録する。

【0075】この配送方法において、配送経路上の盗聴の脅威を考えた場合、配送経路上を流れるデータはK2とK1暗号化情報固有鍵Ec (K1, Kc) であり、配送用共通鍵を知らなければK2からK1を求めることはできず、K1がなければK1暗号化情報固有鍵Ec (K1, Kc) から情報固有鍵Kcは復号できず、情報固有鍵Kcがなければ暗号情報Ec (Kc, C) は復号できないため配送経路上を流れるデータを盗聴されても目的情報Cを復元することができないため、安全である。

【0076】また、実施形態4の方法で記憶メディア1に記録された情報を利用する場合の方法については、実施形態3の情報利用方法と同じであるため、省略する。実施形態4の場合、目的情報Cが大容量の場合でも鍵サーバ9と情報記録装置7の間の通信量は大きくならないため利用者の負担を減らすことができる。

【0077】図5は、本発明の第5の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。同図に示す実施形態5のシステムは、情報固有鍵の利用を省略しつつも書換え不可能なメディアIDを利用することにより複製による不正使用の防止、可搬性の維持、盗聴に対する防御を達成するものである。このシステムは、記憶メディア1と、この記憶メディア1に情報を書き込む情報記録装置2と、記憶メディア1に格納された情報を利用する際に使う情報利用装置3と、情報を配信する鍵サーバ10とから構成され、元の目的情報は情報提供者5から提供される。

【0078】記憶メディア1は、記憶メディア独自のID11と、通常の手換え可能な記憶領域12から構成されている。

【0079】また、記憶メディア1に情報を書き込む情報記録装置2は、公開鍵ペア生成処理部21と情報記録処理部22を有し、記憶メディア1を装着した上で記憶メディア1からの記憶メディア独自のID11の読み出しと、記憶領域12への書き込みを行うことができる。

【0080】情報を配信する鍵サーバ10は、情報提供者5からの目的情報を記憶する記憶装置101と、この記憶装置101に記憶されている目的情報をメディア公開鍵を用いて暗号化する情報暗号化処理部102を有する。情報提供者5からの目的情報は、予め鍵サーバ10に送信され、鍵サーバ10の記憶装置101に記録されている。

【0081】目的情報を鍵サーバ10から記憶メディア1まで配送する場合には、まず記憶メディア1から記憶メディア独自のID11を読み出し、情報記録装置2内

の公開鍵ペア生成処理部21で記憶メディア独自のID11を利用して、メディア公開鍵Kpmとメディア秘密鍵Ksmを生成し、メディア公開鍵Kpmを鍵サーバ10に送信する。メディア公開鍵Kpmを受信した鍵サーバ10は、記憶装置101から目的情報を読み出し、情報暗号化処理部102において目的情報をメディア公開鍵Kpmで暗号化し、暗号情報Ec (Kpm, C) を生成する。

【0082】それから、鍵サーバ10は、暗号情報Ec (Kpm, C) を情報記録装置2に送信する。情報記録装置2は、暗号情報Ec (Kpm, C) を受信すると、情報記録処理部22にて記憶メディア1の記憶領域12に暗号情報Ec (Kpm, C) を記録する。

【0083】この配送方法を利用した配送経路上の盗聴の脅威を考えた場合、配送経路上のデータはメディア公開鍵Kpmと暗号情報Ec (Kpm, C) であり、メディア秘密鍵Ksmがなければ暗号情報Ec (Kpm, C) を復号できないため、メディア公開鍵Kpmが盗聴されても問題がない。従って、配送経路上を流れるデータを盗聴されても目的情報Cを復元することはできず、安全である。

【0084】次に、実施形態5において記憶メディア1に記録された情報を利用する方法について説明する。情報利用装置3は、公開鍵ペア生成処理部31、情報復号処理部33、および情報利用処理部34を有し、記憶メディア1を装着した上で記憶メディア1からの記憶メディア独自のID11の読み出しと、記憶領域12からの読み出しを行うことができる。なお、公開鍵ペア生成処理部31は情報記録装置2の公開鍵ペア生成処理部21と同じアルゴリズムを用いて、公開鍵および暗号鍵の生成を行うものである。

【0085】情報の配送後、情報を利用する場合、記憶メディア1は情報記録装置2から取り出され、情報利用装置3に装着されているものとする。

【0086】情報を利用する際には、まず記憶メディア1から記憶メディア独自のID11を読み出し、情報利用装置3内の公開鍵ペア生成処理部31で記憶メディア独自のID11を利用して、メディア公開鍵Kpmとメディア秘密鍵Ksmを生成し、情報復号処理部33にメディア秘密鍵Ksmを渡す。鍵復号処理部32は、記憶メディア1の記憶領域12から暗号情報Ec (Kpm, C) を読み出し、この暗号情報Ec (Kpm, C) をメディア秘密鍵Ksmで復号して、目的情報Cを得て、情報利用処理部34に渡す。情報利用処理部34は、目的情報Cを利用するための処理を行うものであり、ここではその処理は規定しないが、例えば音楽、動画像、静止画像、テキスト等の各種情報の再生等が考えられる。

【0087】ここで不正利用者が記憶メディア1から暗号信号Ec (Kpm, C) を読み出し、別の記憶メディア1に複製する場合を考える。この時、別の記憶メディア

アには記憶メディア独自のIDがあるが、これは書換えができないため複製することはできない。複製した記憶メディアを用いて、情報利用装置で情報を利用しようとした場合、公開鍵ペア生成処理部31ではメディア公開鍵 K_{pm}' とメディア秘密鍵 K_{sm}' が生成されるが、このメディア秘密鍵 K_{sm}' では暗号情報 $E_c(K_{pm}, C)$ を復号することはできない。このため、暗号情報 $E_c(K_{pm}, C)$ から目的情報 C を復号することもできず、結局複製した記憶メディアでは目的情報を利用することはできないため、情報を不正利用することはできない。

【0088】

【発明の効果】以上説明したように、本発明によれば、記憶メディアに記録された情報を複製されても、記憶メディア独自の識別子は複製できないので、複製した暗号化情報固有鍵から情報固有鍵を復号することはできず、従って暗号化情報から目的情報を復号することができず、不正に複製を取っても目的情報の不正利用はできない。

【0089】また、本発明によれば、通信中の情報が盗聴された場合でも、メディア公開鍵、暗号化情報固有鍵、暗号化情報から目的情報を復号することができず、安全に情報を配送することができる。

【0090】更に、本発明によれば、目的情報は記憶メディアに記憶され持ち運びが容易にできるので、目的情報の可搬性を上げることができる。

【0091】本発明によれば、一般に公開鍵暗号方式の復号処理よりも共通鍵暗号の復号処理の方が処理量が少なく、暗号化情報よりも暗号化情報固有鍵が十分小さい場合に、暗号化情報の復号に公開鍵暗号方式を用いる手法よりも処理量を減らすことができる。

【0092】また、本発明によれば、情報固有鍵を用いずにメディア公開鍵で暗号化された暗号化情報を復号するにはメディア秘密鍵が必要であり、メディア秘密鍵は記憶メディア独自の識別子から生成されるので、記憶メディアから暗号化情報が別の記憶メディアに複製されても、別の記憶メディア独自の識別子から生成されるメディア秘密鍵では暗号化情報を復号できず、従って情報の複製による不正利用を防止することができる。

【0093】更に、本発明によれば、情報記録装置からサーバに送信される情報はメディア公開鍵のみであり、メディア公開鍵は記憶メディア独自の識別子から生成さ

れるものであるので、通信中に盗聴されても不正利用できない。また、サーバから情報記録装置に送信される目的情報はメディア公開鍵で暗号化されており、メディア秘密鍵は記憶メディア独自の識別子から生成されるので、通信中に盗聴されても不正利用できない。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

【図2】本発明の第2の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

【図3】本発明の第3の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

【図4】本発明の第4の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

【図5】本発明の第5の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

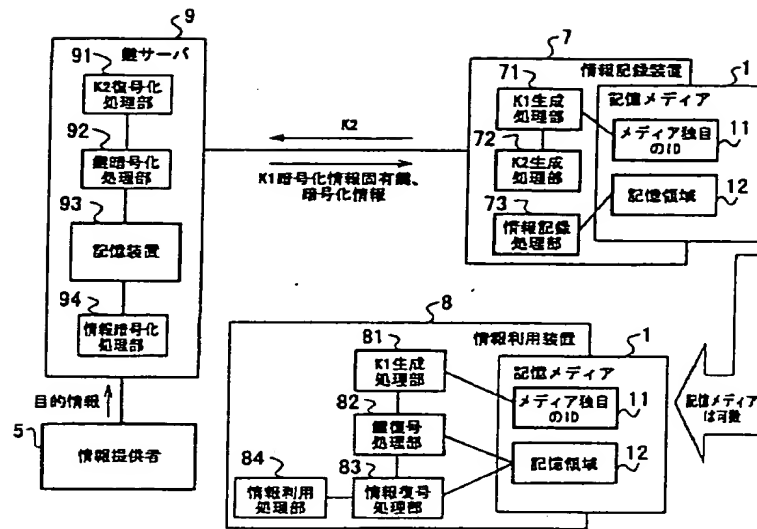
【符号の説明】

- 1 記憶メディア
- 2 情報記録装置
- 3 情報利用装置
- 4 鍵サーバ

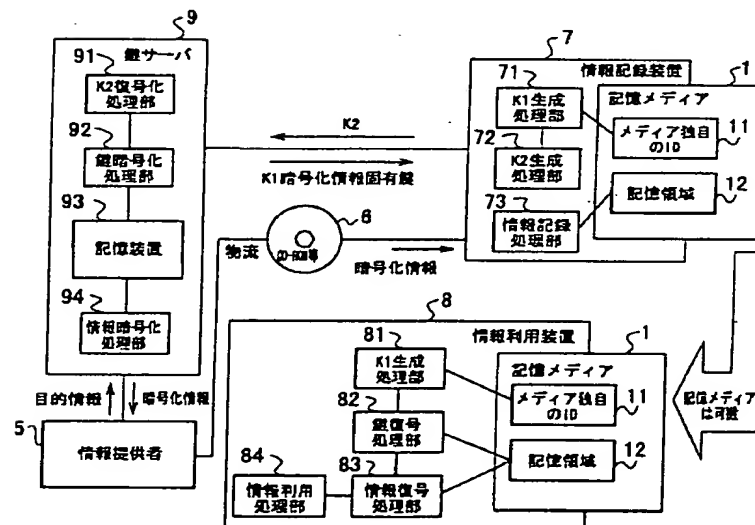
- 11 記憶メディア独自のID
- 12 記憶領域
- 21, 31 公開鍵ペア生成処理部
- 22 情報記録処理部
- 32 鍵復号処理部
- 33 情報復号処理部
- 34 情報利用処理部
- 41 公開鍵暗号化処理部
- 42 記憶装置
- 43 情報暗号化処理部

Figure 1 is a block diagram of the information processing system 100. The system includes a server 4, a recording device 2, and an information utilization device 3. The server 4 consists of a public key encryption processing unit 41, a recording unit 42, and a decryption processing unit 43. The recording device 2 consists of a public key generation processing unit 21, an information recording processing unit 22, a memory medium 11, and a memory area 12. The information utilization device 3 consists of a public key generation processing unit 31, a decryption processing unit 32, an information utilization processing unit 34, an information encryption processing unit 33, a memory medium 11, and a memory area 12. The server 4 and the recording device 2 are connected via a media connection line. The recording device 2 and the information utilization device 3 are connected via a communication line 6. The server 4 and the information utilization device 3 are connected via a network 5. The server 4 sends encrypted information to the recording device 2, which records it on the memory medium 11. The information utilization device 3 retrieves the information from the memory medium 11 and sends it back to the server 4 via the network 5.

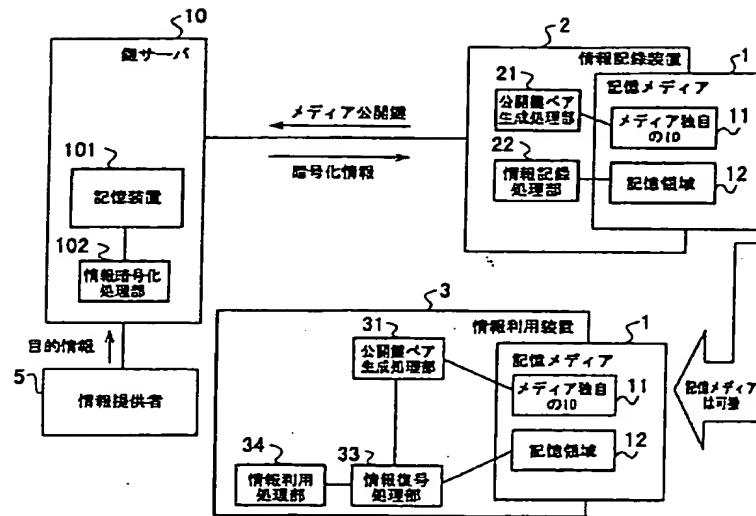
【図 3】



【図 4】



【図 5】



フロントページの続き

(72)発明者 三宅 延久

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 庵 祥子

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 有田 一穂

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

Fターム(参考) 5B017 AA06 AA07 BA05 BA07 BB02
BB07 CA09 CA15 CA16

5J104 AA12 AA16 EA16 EA17 EA22
EA26 NA02 NA36 NA37 PA07
PA14

9A001 EE03